"Express Mail" mailing label number:

EV 335894829 US

ENHANCED NETWORK MANAGEMENT SYSTEM

Ken R. Jones
Brian A. Gonsalves

CROSS-REFERENCE TO RELATED APPLICATION(S)

[1001] The present invention is related to subject matter that is disclosed in U.S. Pat. No. _____, filed on the same day as the present patent application, entitled "ENHANCED CSU/DSU (CHANNEL SERVICE UNIT/DATA SERVICE UNIT)," naming Ken R. Jones and Brian A. Gonsalves as inventors, and incorporated herein by reference in its entirety.

BACKGROUND

Field of the Disclosure

[1002] The present disclosure relates generally to network management systems and methods of collecting management information data.

Description of the Related Art

[1003] Communication nodes located between wide area networks and local area data networks have been deployed commercially. An example of a communication node is a channel service unit/data service unit (CSU/DSU). CSU/DSU units that are currently available for deployment receive and forward data traffic between a wide area network and a local area network.

[1004] Network management systems typically rely on CSU/DSU units to monitor networks and equipment. Network management systems can be connected to a wide area network and may collect management reports from multiple CSU/DSU units via the wide area network. Network management systems use such collected information to

administer service level agreements, monitor equipment, and the like. Some of the network equipment is owned and operated by customers and other equipment is owned and operated by a service provider, such as a telecommunications company. Customer billing can be based on a guaranteed minimum throughput and/or a local loop charge. For proper billing and to determine and allocate customer billing credits, network management system operators need information that differentiates between customer equipment faults and service provider outages.

[1005] CSU/DSU units are often connected directly to a wide area network via asynchronous transfer mode (ATM) equipment, but in some implementations the CSU/DSU unit may transfer frame relay communications to an intermediate network in the communication path to the wide area network. The intermediate network is typically transparent to the CSU/DSU unit. Depending on the connection to the wide area network, some CSU/DSU units are not capable of monitoring the intermediate connection used to transfer the data traffic. Lack of network management information is problematic when implementing service level agreements where customers are charged based on data bandwidth on the transparent connection.

[1006] Accordingly, there is a need for an enhanced method of accessing management data for transparent connections or networks.

BRIEF DESCRIPTION OF THE DRAWINGS

[1007] FIG. 1 is a general diagram that illustrates a network management system for a data network according to an embodiment of the present disclosure.

[1008] FIG. 2 is a block diagram of an embodiment of the network management system of FIG. 1.

[1009] FIG. 3 is a flow chart that illustrates operation of the network management system of FIG. 1.

[1010] The use of the same reference symbols in different drawings indicates similar or identical items.

DESCRIPTION OF THE EMBODIMENT(S)

[1011] An enhanced network management system is disclosed. The network management system is configured to receive management information via multiple virtual connections from multiple data communication nodes. The management information includes service level information for a transparent connection, for example, a Digital Subscriber Line (DSL) connection carrying encapsulated frame relay packets between two networks, for example a wide area network and a local area network. The transparent connection is intermediate to the wide area network and the local area network. The management information further includes equipment failure information of customer equipment, for example, a bridging node used to encapsulate the frame relay packets. Thus, using the collected management information, a network outage caused by customer equipment failure can be differentiated from a service provider service level event.

[1012] FIG. 1 is a general diagram that illustrates a network management system of a data network according to an embodiment of the present disclosure. A network management system 102 is connected to a wide area network 104. Multiple local area networks 106 are coupled to wide area network 104 through data communication nodes 108, bridges 110, digital subscriber line access multiplexers (DSLAMs) 112 and asynchronous transfer mode (ATM) devices 114. Other local area networks 116 are coupled to wide area network 104 via data communication nodes 118.

[1013] As illustrated, data traffic flows between local area networks via their connections to the wide area network. For example, data traffic from a first local area network 106 flows to a second local area network 106 via a first data communication node 108, a first bridge 110, a first DSLAM 112, a first ATM 114 through wide area network 104 and back through the first ATM 114, the first DSLAM 112, to a second bridge 110 and a second data communication node 108. Data communication nodes 106 communicate with wide area network 104 according to a frame relay type protocol. A frame relay type protocol is a packet-switching protocol for connecting devices on a wide area network. Transparent to the communication between the data communication nodes 108 and wide

area network 104, corresponding bridges 110 transfer encapsulated data traffic to DSL connections 111 to DSLAMs 112. The data traffic is encapsulated according to Frame Relay Over DSL protocol. Note that bridges 110 and DSLAMs 112 encapsulate and de-capsulate the frame relay traffic and do not interpret or re-route the traffic. For example, a more direct communication path between the first local area network 106 and the second local area network 106 would not include the first ATM 114 and wide area network 104.

[1014] Wide area network 104 can be, for example, the Internet. Local area networks 106 can include, for example, a router and various peripheral equipment end terminals coupled via an Ethernet connection. Alternatively, local area network 106 can include a modem connected to a home user computer system.

[1015] Network management system 102 administers, among other things, service level agreements for DSL connections 111. Because equipment failures in customer owned bridges 110 could affect service levels on service provider owned DSL connections 111, network management system 102 must be capable of differentiating between service provider outages and equipment failures. As illustrated, management information flows from bridges 110 to corresponding data communication nodes 108 that monitor equipment fault information for bridges 110 and service level information for DSL connections 111. The management information then flows to network management system 102 via bridge 110, DSLAM 112, ATM equipment 114, and wide area network 104.

[1016] DSL connections 111 are high-speed digital connections. Each customer's traffic is bridged on to a separate Data Link Connection Identifier (DLCI). A DLCI is a private or switched virtual circuit in a Frame Relay network that indicates how the data is to be routed. By transferring traffic data using DSL connections 111, service costs are reduced and penetration is increased into certain markets that can be economically reached without the added expense of Frame Relay Switches in remote offices.

[1017] Data communication nodes 108 have management agents responsible for performing network management functions and can determine outage errors on DSL

connections 111. The data nodes 108 can also differentiate between equipment failure of customer owned bridges 110 and service level or network failure of provider owned DSL connections 111. Data communication nodes 108 can monitor bridges 110 and DSL connections 111 utilizing a frame relay virtual circuit or connection (VC) or a DLCI. A VC is a two-way connection between the CSU/DSU 110 and bridging node 112 that communicates Simple Network Management Protocol (SNMP). SNMP is an Internet standard protocol, defined in RFC 1157, developed to manage nodes on an IP network.

[1018] Information gathered by data communication nodes 108 is sent to network management system 102 across wide area network 104 using another virtual circuit. Thus, bridges 110 send management information to data communication nodes 108 and the information is forwarded to network management system 102. The information can be sent in SNMP or Common Reliable Accounting for Network Element (CRANE) format, without additional processing. Network management system 102 formats collected information and performs calculations for performance measurements and bandwidth guarantees.

[1019] FIG. 2 is a block diagram of an embodiment of the network management system 102. Network management system 102 includes a router 202 for connection to a wide area network, a middleware server 204 and a report collector 206. Middleware server 204 is a repository for management information collected from various data communication nodes. Report collector 206 can provide analysis of management information, provide notification of equipment failures, and provide administration of service level agreements for multiple customers.

[1020] FIG. 3 is a flow chart that illustrates operation of the network management system 102. Management information is collected for a transparent connection, such as a DSL connection, carrying encapsulated data traffic, at step 302. The data traffic can be according to a frame relay protocol and the encapsulated data traffic can be according to a frame relay over DSL protocol. The transparent connection can be an intermediate network, for example, a DSL connection, between a local area network and a wide area network. Equipment failure information, such as failure of customer equipment, is

identified using the collected management information, at step 304. Service level agreement violations, such as DSL bandwidth failures, may be identified using the collected management information, at step 306. Thus, using the collected management information, a network outage caused by customer equipment failure can be differentiated from a service provider service level event. Service level information can be presented to a customer, at step 308. Detected equipment failures can be presented to a customer, at step 310.

[1021] The above-disclosed subject matter is to be considered illustrative, and not restrictive, and the appended claims are intended to cover all such modifications, enhancements, and other embodiments, which fall within the true spirit and scope of the present invention. Thus, to the maximum extent allowed by law, the scope of the present invention is to be determined by the broadest permissible interpretation of the following claims and their equivalents, and shall not be restricted or limited by the foregoing detailed description.